

Hon. Joseph A. Marutollo U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
*Printed name and title***Print****Save As...****Reset**

ATTACHMENT A

Property to Be Searched

The property to be searched is:

- (1) One 4 GB Kingston SD Card;
- (2) Six (6) USB flash drives;
- (3) Samsung Galaxy watch with black straps;
- (4) Dell Latitude 5590 laptop, No. 25650703802;
- (5) Seagate external hard drive, P/N IK9AP6-501;
- (6) Samsung model cellphone with IMEI No. 351518945352256/01 and IMEI2 No. 351681915352258/01;
- (7) Apple iPhone with IMEI No. 357631096484234/01 and IMEI2 No. 357632096484232/01;
- (8) Samsung SM-J320FN cellphone with IMEI No. 355099088222438;
- (9) Toshiba Portege R300 Laptop, serial no. 88029479H;
- (10) Cromax X1800 cellphone with IMEI Nos. 911481400403598, 911481400403606, and SIM card Nos. 89701013958022120647 and 897010210953878537;
- (11) Philips Xenium E311 cellphone with IMEI Nos. 866635024442572 and 866635027192570 and Elise SIM card No. EE21220123062206;
- (12) Samsung SM-G920F cellphone with IMEI No. 359937067052258;
- (13) Sony Ericsson LT18i cellphone with IMEI No. 351870057473267;
- (14) Tele2 SIM-card case with IMSI No. 89372038005053487270;
- (15) ZTE-G S202 cellphone with IMEI No. 868663001743653 and ELISA SIM card No. EE21170815376853;
- (16) Silicon Power 4GB SD memory card;
- (17) myPhone 3320 cellphone with IMEI Nos. 354028090104483 and 354028090104491;
- (18) Nokia 8800E-1 cell phone with IMEI No. 358645013721543;
- (19) BQ-3201 cellphone with IMEI Nos. 351614102396465 and 351614102396473, SIM card with IMSI No. 897010210782518668;
- (20) Samsung SM-G925F cell phone with IMEI No. 357460106/573487/8;
- (21) Huawei ATU-L21 cell phone;
- (22) Samsung NP-R509 laptop, serial no. Z9S993FS300637T;
- (23) Acer Aspire 5750 laptop, serial no. LXRL802041 1340187F3400; and

(24) Prestigio MultiPad tablet, serial no. PMP11122405214;

(collectively, the “SUBJECT DEVICES”) that were recovered from the person of VADIM KONOSHCHENOK on or about December 6, 2022, and the residence of VADIM KONOSHCHENOK, located in Tallinn, Estonia, on or about January 7, 2023. The SUBJECT DEVICES are currently in law enforcement possession within the Eastern District of New York.

ATTACHMENT B

Particular Things to be Seized

All information or records on the SUBJECT DEVICES described in Attachment A that relate to violations of the International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1701 et seq.; the Export Control Reform Act (“ECRA”), 50 U.S.C. § 4801 et seq. and related regulations; Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 554 (smuggling goods); Title 18, United States Code, Section 1956 (money laundering); as well as conspiracy to commit such offenses under Title 18, United States Code, Sections 371 and 1349 (collectively, the “Subject Offenses”), committed by or involving VADIM KONOSHCHENOK, since January 1, 2017, including:

- a. Communications or other records between, among, or about KONOSHCHENOK, and other co-conspirators, including individuals whose identities are not yet known, including communications through intermediaries, regarding the Subject Offenses;
- b. Communications or other records between, among, or about academic or scientific researchers, academic or scientific research (including research related to quantum physics, quantum mechanics, and quantum computing), research institutions, funding or payment for research, research being collected or conducted in the United States, or conducting or transferring research or research findings outside of the United States;
- c. Communications or other records between, among, or about officials of universities or research institutions based in Russia, including communications through intermediaries;
- d. Communications or other records between, among, or about individuals or entities or individuals who are employed by or maintain an affiliation with individuals or entities who at any point in time have been placed on the U.S. Department of the Treasury, Office of Foreign Assets Control’s Specially Designated Nationals List;
- e. Communications or other records between, among, or about individuals or entities or individuals who are employed by or maintain an affiliation with individuals or entities who at any point in time have been on the U.S. Department of the Commerce, Bureau of Industry and Security’s Entity List or Military End User List;

- f. Records and other information regarding KONOSHCHENOK and other coconspirators' travel to and from the United States;
- g. Records and other information relating to the physical locations of KONOSHCHENOK and other coconspirators, including Global Positioning System location data, Internet Protocol address information, photographs, videos, audio recordings, and communications;
- h. Copies of documentation or other records from Russian officials or employees or affiliated researchers at academic or research institutions or companies outside of the United States related to the Subject Offenses;
- i. Financial information related to KONOSHCHENOK and other coconspirators' transfer of money, including bank statements, money transfers, tax filings, and communications regarding financial information;
- j. Information relating to knowledge or awareness of law enforcement or government investigations, electronic or physical surveillance by law enforcement, means and methods of evading law enforcement surveillance or of concealing activities from law enforcement or government agencies, and communications discussing whether one or more persons is under surveillance or investigation by law enforcement or government agencies;
- k. Information relating to attempts to alter, destroy, mutilate, or conceal a record, document, or other object, including by destroying physical records, deactivating any Internet account, deleting applications from an electronic device, or concealing an electronic device from law enforcement or other government agencies;
- l. Information relating to any benefit, financial or otherwise, conferred to KONOSHCHENOK, and other co-conspirators for committing the Subject Offenses;
- m. Attribution evidence showing who used or owned the SUBJECT DEVICES at the time the records and information described in this warrant were created, edited, or deleted, including logs, phonebooks, saved usernames and passwords, documents, browsing history, photographs, videos, audio recordings, and messages; and
- n. Evidence indicating the state of mind of KONOSHCHENOK, and other coconspirators, including individuals whose identities are not yet known, as it relates to the crimes under investigation.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form

(such as printing or typing); and any aural or photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

This warrant authorizes a review of electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, language experts and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CRH
F# 2019R01707

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF

- (1) One 4 GB Kingston SD Card;
- (2) Six (6) USB flash drives;
- (3) Samsung Galaxy watch with black straps;
- (4) Dell Latitude 5590 laptop, No. 25650703802;
- (5) Seagate external hard drive, P/N IK9AP6-501;
- (6) Samsung model cellphone with IMEI No. 351518945352256/01 and IMEI2 No. 351681915352258/01;
- (7) Apple iPhone with IMEI No. 357631096484234/01 and IMEI2 No. 357632096484232/01;
- (8) Samsung SM-J320FN cellphone with IMEI No. 355099088222438;
- (9) Toshiba Portege R300 Laptop, serial no. 88029479H;
- (10) Cromax X1800 cellphone with IMEI Nos. 911481400403598, 911481400403606, and SIM card Nos. 89701013958022120647 and 897010210953878537;
- (11) Philips Xenium E311 cellphone with IMEI Nos. 866635024442572 and 866635027192570 and Elise SIM card No. EE21220123062206;
- (12) Samsung SM-G920F cellphone with IMEI No. 359937067052258;
- (13) Sony Ericsson LT18i cellphone with IMEI No. 351870057473267;

TO BE FILED UNDER SEAL

**APPLICATION FOR A
SEARCH WARRANT FOR
ELECTRONIC DEVICES**

Case No. 24-MJ-24

- (14) Tele2 SIM-card case with IMSI No. 89372038005053487270;
- (15) ZTE-G S202 cellphone with IMEI No. 868663001743653 and ELISA SIM card No. EE21170815376853;
- (16) Silicon Power 4GB SD memory card;
- (17) myPhone 3320 cellphone with IMEI Nos. 354028090104483 and 354028090104491;
- (18) Nokia 8800E-1 cell phone with IMEI No. 358645013721543;
- (19) BQ-3201 cellphone with IMEI Nos. 351614102396465 and 351614102396473, SIM card with IMSI No. 897010210782518668;
- (20) Samsung SM-G925F cell phone with IMEI No. 357460106/573487/8;
- (21) Huawei ATU-L21 cell phone;
- (22) Samsung NP-R509 laptop, serial no. Z9S993FS300637T;
- (23) Acer Aspire 5750 laptop, serial no. LXRL802041 1340187F3400;
AND,
- (24) Prestigio MultiPad tablet, serial no. PMP11122405214;

CURRENTLY LOCATED IN THE EASTERN
DISTRICT OF NEW YORK

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nicholas Milan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic

devices, described below and in Attachment A—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been since 2018. I am currently assigned to investigate export control violations and espionage by foreign governments and related criminal and counterintelligence activity. Through my training, education, and experience, I am familiar with the techniques and methods of operation used by individuals involved in intelligence and criminal activities to conceal their behavior from detection by law enforcement authorities. I have participated in numerous investigations, during the course of which I have conducted physical and electronic surveillance, interviewed witnesses, examined financial records, executed court-authorized search warrants and used other techniques to secure relevant information.

3. The facts in this affidavit come from my personal observations, my training and experience, my review of documents and records, and information obtained from other law enforcement agents. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Where the content of statements, conversations and documents are described herein, they are done so in pertinent part and in sum and substance.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is: (1) one 4 GB Kingston SD Card that was recovered from VADIM KONOSHCHENOK following a border stop by Estonian authorities on October 27, 2022 (the “BORDER STOP DEVICE”); (2) Six (6) USB flash drives; (3) Samsung Galaxy watch with black straps; (4) Dell Latitude 5590 laptop, No. 25650703802; (5) Seagate external hard drive,

P/N IK9AP6-501; (6) Samsung model cellphone with IMEI No. 351518945352256/01 and IMEI2 No. 351681915352258/01; and (7) Apple iPhone with IMEI No. 357631096484234/01 and IMEI2 No. 357632096484232/01 that were recovered from VADIM KONOSHCHENOK following his arrest by Estonian authorities on December 6, 2022 (the “POST-ARREST DEVICES”), as well as (8) Samsung SM-J320FN cellphone with IMEI No. 355099088222438; (9) Toshiba Portege R300 Laptop, serial no. 88029479H; (10) Cromax X1800 cellphone with IMEI Nos. 911481400403598, 911481400403606, and SIM card Nos. 89701013958022120647 and 897010210953878537; (11) Philips Xenium E311 cellphone with IMEI Nos. 866635024442572 and 866635027192570 and Elise SIM card No. EE21220123062206; (12) Samsung SM-G920F cellphone with IMEI No. 359937067052258; (13) Sony Ericsson LT18i cellphone with IMEI No. 351870057473267; (14) Tele2 SIM-card case with IMSI No. 89372038005053487270; (15) ZTE-G S202 cellphone with IMEI No. 868663001743653 and ELISA SIM card No. EE21170815376853; (16) Silicon Power 4GB SD memory card; (17) myPhone 3320 cellphone with IMEI Nos. 354028090104483 and 354028090104491; (18) Nokia 8800E-1 cell phone with IMEI No. 358645013721543; (19) BQ-3201 cellphone with IMEI Nos. 351614102396465 and 351614102396473, SIM card with IMSI No. 897010210782518668; (20) Samsung SM-G925F cell phone with IMEI No. 357460106/573487/8; (21) Huawei ATU-L21 cell phone; (22) Samsung NP-R509 laptop, serial no. Z9S993FS300637T; (23) Acer Aspire 5750 laptop, serial no. LXRL802041 1340187F3400; and, (24) Prestigio MultiPad tablet, serial no. PMP11122405214 that were recovered from the residence of VADIM KONOSHCHENOK, located in Tallinn, Estonia on or about January 7, 2023 (the “PREMISES DEVICES”) (collectively, with the POST-ARREST DEVICES, the “SUBJECT DEVICES”). The SUBJECT DEVICES were provided to U.S. law enforcement by Estonian

authorities. The SUBJECT DEVICES are currently in law enforcement possession within the Eastern District of New York.

5. The Supreme Court and other lower courts have held that neither the Fourth Amendment's warrant requirements nor its exclusionary rule is applicable to searches and seizures conducted by foreign law enforcement, even when those searches and seizures are done at the request of the United States government. See, e.g., United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (holding that Fourth Amendment has no application to search conducted by U.S. authorities of a location located in Mexico belonging to a Mexican citizen and resident); United States v. Getto, No. 09 CR 667 HB, 2010 WL 3467860, at *3 (S.D.N.Y. Aug. 25, 2010), aff'd, 729 F.3d 221 (2d Cir. 2013) (finding that Fourth Amendment did not apply even where foreign government actions were requested by U.S. authorities pursuant to MLAT). Nonetheless, the government seeks this warrant to search the SUBJECT DEVICES out of an abundance of caution.

6. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B. As described herein, there is probable cause that the SUBJECT DEVICES contain evidence and instrumentalities of violations of, inter alia, the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701 et seq.; the Export Control Reform Act ("ECRA"), 50 U.S.C. § 4801 et seq. and related regulations; Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 554 (smuggling goods); Title 18, United States Code, Section 1956 (money laundering); as well as conspiracy to commit such offenses under Title 18, United States Code, Sections 371 and 1349 (collectively, the "Subject Offenses"), committed by KONOSHCHENOK and others.

RELEVANT STATUTORY BACKGROUND

I. The International Emergency Economic Powers Act

7. IEEPA, 50 U.S.C. §§ 1701-1706, authorizes the President of the United States to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat. Pursuant to the authority under IEEPA, the President and the executive branch have issued orders and regulations governing and prohibiting certain transactions with certain countries, entities, and individuals by U.S. persons or involving U.S.-origin goods. Under IEEPA, it is a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any regulation promulgated thereunder, including the sanctions regulations described below. See 50 U.S.C. § 1705.

8. In 2014, pursuant to the IEEPA, the President issued Executive Order 13660, which declared a national emergency with respect to the situation in Ukraine. See Exec. Order No. 13660 (Mar. 6, 2014), 79 Fed. Reg. 13,493 (Mar. 10, 2014). This national emergency has remained in continuous effect since 2014. Executive Order 13660 found that the actions and policies of certain persons asserting governmental authority in the Crimean region without the authorization of the Government of Ukraine constituted an unusual and extraordinary threat to the national security and foreign policy of the United States. See id. To address this national emergency, the President, among other things, prohibited U.S. persons from engaging in certain transactions with individuals determined by the Secretary of the Treasury to meet one or more enumerated criteria. See id. §§ 1, 4.

9. Specifically, Executive Order 13660 blocks the property and interests in property of designated persons and provides that the blocking of any such property and interests in property includes a prohibition on engaging in certain transactions with any such designated person, as

described herein. In 2014, the President issued several additional Executive Orders that address the national emergency declared in Executive Order 13660. See Exec. Order No. 13661 (Mar. 16, 2014), 79 Fed. Reg. 15,535 (Mar. 19, 2014); Exec. Order No. 13662 (Mar. 20, 2014), 79 Fed. Reg. 16,169 (Mar. 24, 2014); and Exec. Order No. 13685 (Dec. 19, 2014), 79 Fed. Reg. 77,357 (Dec. 24, 2014) (together with Executive Order 13660, the Ukraine-Related Executive Orders). Among other things, the Ukraine-Related Executive Orders expand upon Executive Order 13660 by blocking the property and interest in property of additional individuals and entities related to Ukraine and the Crimea region of Ukraine, defining additional prohibited transactions, and setting forth additional criteria that the Secretary of the Treasury may use in designating blocked persons and entities.

10. To implement Executive Order 13660, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued the Ukraine-Related Sanctions Regulations. See generally 31 C.F.R. part 589. These regulations incorporate by reference the definition of prohibited transactions set forth in the Ukraine-Related Executive Orders. See 31 C.F.R. § 589.201. The regulations also provide that the names of persons designated by OFAC pursuant to the Ukraine-Related Executive Orders, whose property and interests are therefore blocked, are published in the Federal Register and incorporated into the Specially Designated Nationals ("SDN") and Blocked Persons List (the "SDN List"), which is published on OFAC's website. See id. note 1.

11. The Ukraine-Related Sanctions Regulations prohibit conspiring to and attempting to evade, avoid, or violate the regulations. The prohibitions further include the unauthorized export of goods from the United States to a third country if the goods are intended or destined for banned entities in Russia. Willful violations of sanctions regulations constitute criminal offenses under

IEEPA and carry a 20-year maximum term of imprisonment and up to a \$1,000,000 fine. See 50 U.S.C. § 1705(c).

II. The ECRA and Export Administration Regulations

12. The Export Administration Regulations (“EAR”), 15 C.F.R. §§ 730-774, which were promulgated by the U.S. Department of Commerce (“DOC”), Bureau of Industry and Security (“BIS”), regulate the export of goods, technology, and software from the United States. Under the ECRA, it is a crime to violate, attempt to violate, conspire to violate, or cause a violation of any regulation, order, license, or authorization issued pursuant to the statute, including the EAR. See 50 U.S.C. § 4819(a)(1). Willful violations of the EAR constitute criminal offenses under the ECRA and carry a 20-year maximum term of imprisonment and up to a \$1,000,000 fine. See 50 U.S.C. § 4819(b).

13. Through the EAR, the BIS reviews and controls the export from the United States to foreign countries of certain U.S. items. See 15 C.F.R. §§ 734.2-.3. In particular, the BIS has placed restrictions on the export and re-export of items that it has determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depend on several factors, including the technical characteristics of the item, the destination country, the end user and the end use.

14. The most sensitive items subject to the EAR controls are identified on the Commerce Control List (“CCL”), set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1. Items listed on the CCL are categorized by Export Control Classification Number (“ECCN”), each of which is subject to export control requirements depending on destination, end use and end user.

15. The BIS publishes the names of certain foreign persons – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. These persons comprise the Entity List, which is found at Title 15, Code of Federal Regulations, part 774, Supplement Number 4. The persons on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR, due to a determination that such persons have engaged in activities contrary to U.S. national security and/or foreign policy interests.

PROBABLE CAUSE¹

I. Introduction

16. U.S. law enforcement, including the FBI, is prosecuting and investigating a scheme involving KONOSHCHENOK, Boris Livshits, Yevgeniy Grinin, Alexey Ippolitov, Svetlana Skvortsova, Alexey Brayman, Vadim Yermolenko, Nikolaos Bogonikolos and others, known and unknown (collectively, the “Subject Individuals”), for violating export control laws by shipping dual-use, military-grade items and sensitive technologies from U.S. businesses to end users in the Russian Federation, including the Russian government and sanctioned entities, as part of the “Serniya Network.”

17. On May 22, 2023, a grand jury in the Eastern District of New York returned a second superseding indictment charging KONOSHCHENOK, along with the other Subject Individuals, with a variety of criminal offenses related to this scheme. See United States of America v. Yevgeniy Grinin, et al., Case Number 22-CR-409 (S-2) (HG). KONOSHCHENOK is charged in the superseding indictment with Conspiracy to Defraud the United States, in violation

¹ All translations from Russian to English are in draft form and subject to change.

of Title 18, United States Code, Section 371 (Count One); Conspiracy to Violate the Export Control Reform Act (“ECRA”), in violation of Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) (Count Fourteen); and Smuggling Goods from the United States, in violation of Title 18, United States Code, Section 554(a) (Count Fifteen).

18. As discussed further below, the evidence reflects that KONOSCHENOK was responsible for receiving items that were illegally obtained and exported from the United States, and then smuggling those items into Russia. KONOSCHENOK used electronic communications to help facilitate his role in the scheme. KONOSCHENOK was stopped by Estonian authorities on October 27, 2022, while attempting to cross into Russia, and found with, among other things, the BORDER STOP DEVICE. KONOSCHENOK was arrested on December 6, 2022, and was found in possession of, among other things, the POST-ARREST DEVICES. After KONOSCHENOK’s arrest, Estonian authorities conducted a search of KONOSCHENOK’s Estonian residence, and seized, among other things, the PREMISES DEVICES.

II. The Serniya Network and the Subject Individuals

19. OOO² Serniya Engineering (“Serniya”) and OOO Sertal (“Sertal”) are wholesale machinery and equipment companies based in Moscow, Russia. Serniya headed an illicit procurement network operating under the direction of Russia’s intelligence services (collectively, the “Serniya Network”), which evaded U.S. and Western sanctions to acquire sensitive military grade and dual use technologies, including advanced semiconductors, for the Russian military, defense sector, intelligence agencies and research institutions. Sertal operated within the Serniya Network and in turn utilized a network of front companies, shell entities, and bank accounts

² “OOO” is the abbreviation for the Russian business entity type, “общество с ограниченной ответственностью,” which means limited private company and is roughly the equivalent of a limited liability company or LLC in the United States.

throughout the world, including in the United States, to source, purchase, and ship export-controlled items from the U.S. to Russia. Sertal was an accredited contractor by the Russian Federal Security Service (“FSB”), authorized to conduct highly sensitive and classified procurement activities.

20. On or about March 3, 2022, Serniya and Sertal were added to the Entity List. BIS indicated that Serniya, Sertal, and other entities were sanctioned because they “have been involved in, contributed to, or otherwise supported the Russian security services, military and defense sectors, and military and/or defense research and development efforts.” 87 Fed. Reg. 13141. BIS adopted a “policy of denial” with respect to Serniya and Sertal, indicating that BIS would not permit a license to export items to Serniya or Sertal. On or about March 31, 2022, OFAC designated Serniya, Sertal, and several other entities in the Serniya Network and added them to the SDN List. According to OFAC’s press release, the designation was part of “its crackdown on the Kremlin’s sanctions evasion networks and technology companies, which are instrumental to the Russian Federation’s war machine.” OFAC described Serniya as “the center of a procurement network engaged in proliferation activities at the direction of Russian Intelligence Services.”

21. The Subject Individuals were participants in the Serniya Network. The following paragraphs briefly summarizes the evidence of their roles in the scheme.³

a. Ippolitov is a Russian national who resides in Russia and is affiliated with a Russian research institute tied to the Russian state space corporation ROSCOSMOS, and a second Russian institute that was placed on the Entity List in 2022. Ippolitov acted as a liaison

³ A more detailed summary of the evidence of the Subject Individuals’ roles can be found in an affidavit in support of a search warrant for information in Apple Inc. and Yahoo Inc. accounts associated with KONOSHCHENOK, Ippolitov, Yermolenko and Livshits, which is attached hereto as Exhibit 1, and incorporated by reference. See 22-M-1285 (RML).

between Serniya and Sertal and Russian end users in the defense and technology sectors. He solicited orders from Russian end users who sought to acquire a particular item or part from the United States, and then relayed the request to employees at Sertal and Serniya, including Grinin and Skvortsova, who were tasked with procuring the desired component from U.S. companies. Ippolitov oversaw the purchase and shipping of the items from U.S. companies through the Serniya Network's front companies and bank accounts.

b. Grinin is a "leader, official, senior executive officer, or member of the board of directors" of Photon Pro LLP, whose property and interests are blocked pursuant to Executive Order 14,024 since April 15, 2021.⁴ On March 9, 2022, Grinin was also added to the BIS Entity List. Skovortsova is a Russian national who works for Sertal as Advisor to the General Director under the supervision of Grinin. Grinin and Skvortsova decided how to fulfill orders placed by Russian end users, including those orders placed through Ippolitov. Grinin and Skvortsova secured funding and shipping for the transactions, as well as assisted in preparing documents with false and misleading information in furtherance of the scheme.

c. Livshits is a Russia-based procurement agent and owner of the U.S. based companies Advanced Web Services LLC and Strandway LLC, which act as front entities for Sertal. Livshits was often tasked by Grinin and Skvortsova to interface directly with the U.S. companies and purchase items requested by Russian end users. In doing so, Grinin, Skvortsova and Livshits discussed methods to evade U.S. export controls and other criminal laws. Livshits also counseled breaking up larger orders to avoid detection by law enforcement. Livshits, who spoke English, communicated with U.S. companies through in-person meetings, telephonic

⁴ See "Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War," available at <https://home.treasury.gov/news/press-releases/jy0692>.

conversations and in email and text exchanges. In those communications, Livshits misrepresented and omitted material information, including information about how the item would be used, the various parties involved in the transaction, and the identity of the ultimate Russian end user.

d. Brayman, a New Hampshire resident, acted as an intermediary, coordinating with Livshits as part of the scheme to evade sanctions and commit the Subject Offenses. Brayman would receive and send packages containing sensitive, dual-use components to other individuals within the Serniya network. Livshits and Brayman repeatedly used Brayman's residence in New Hampshire as a transshipment point for repackaging sensitive military-grade and export-controlled items and forwarding them to intermediate locations in Europe and Asia, from where they were transshipped to Russia.

e. Yermolenko, a New Jersey resident, facilitated the Subject Offenses by obtaining Employee Identification Numbers issued by the Internal Revenue Service; opening and managing bank accounts and shell companies for Livshitz; facilitating illicit money movements; and falsely completing business records, among other acts.

III. KONOSHCHENOK's Involvement in the Criminal Scheme

22. KONOSHCHENOK, while acting under the direction of Livshits, shipped or physically smuggled U.S.-origin items from Estonia to Russia, including dual-use electronics and other export-controlled items.

23. For example, according to shipping and other records, on September 21, 2022, Brayman sent a package from his New Hampshire residence to "Vadim Konoshchenok" at an address in Tallinn, Estonia and a company "Stonebridge Resources." The invoice described the contents as a "Prototype Development Board with Case," manufactured by a software company in Texas and controlled by the DOC under ECCN 3A992.a, which are controlled for anti-terrorism reasons.

24. As another example, on April 27, 2022, Livshits sent an email to himself with KONOSHCHENOK's bank account information. Subsequent emails document a payment of 2,600 Euros to KONOSHCHENOK's bank account, number EE217700771000881710.

25. On May 3, 2022, Livshits received information reflecting showing a package being shipped to an entity in Tallinn, with the recipient listed as KONOSHCHENOK.

26. On October 27, 2022, KONOSHCHENOK was stopped by police and border guard officers in Narva, Estonia, where he was attempting to cross from Estonia into Russia. Inside of KONOSHCHENOK's vehicle were approximately 35 different types of semiconductors and other electronic components, at least four of which were of U.S.-origin and controlled by the DOC under ECCN 3A992.a, for anti-terrorism reasons. Amongst the documents were invoices from a California-based electronics distributor for export controlled electronics, which falsely stated that they were destined for an Estonian end user. According to email and other business records, one of the items had been purchased by co-defendant Livshits and shipped to KONOSHCHENOK on October 18, 2022. The item is used to measure radio frequency and other electronic signals, is of U.S. origin, and is ECCN 3A992.A and controlled for export for counter-terrorism reasons. KONOSHCHENOK was also found in possession of the BORDER STOP DEVICE.

27. Also secreted in KONOSHCHENOK's vehicle were thousands of 6.5mm bullets manufactured by a Nebraska-based firearms components and manufacturing company. The bullets were suitable for a sniper rifle and controlled by BIS under ECCN 0A505.x. According to the Form BIS-711 documents filed with the DOC in accordance with the export of the sniper rounds, these bullets had ostensibly been sold to Germany, Finland, Luxembourg and Latvia but did not disclose their ultimate re-export to Russia.

28. On November 24, 2022, the defendant KONOSHCHENOK was again stopped by police and border guard officers in Narva, Estonia, where he was attempting to cross from Estonia into Russia. Inside of KONOSHCHENOK's vehicle were approximately twenty cases of U.S.-origin bullets controlled under ECCN 0A505.x, including tactical bullets and .338 military sniper rounds of ammunition.

IV. KONOSHCHENOK's Use of Electronic Communications to Further the Conspiracy

29. KONOSHCHENOK participated in the conspiracy, and furthered the criminal scheme, through electronic communications with other members of the conspiracy.

30. These electronic communications—in addition to other evidence such as invoices and business records seized from KONOSHCHENOK's vehicle during the October 27 and November 24 attempted border crossings—revealed that KONOSHCHENOK employed an Estonian front company called “Stonebridge Resources” in furtherance of the scheme. KONOSHCHENOK communicated with Livshits; an individual saved as “Ivan Bullets” in his telephone contacts; and others regarding sourcing, transporting and paying for the ammunition.

31. For example, in one text message, KONOSHCHENOK explicitly stated to “Ivan Bullets” that he will “take the other car, the bullets, the shell casings” and transport them into Russia.

32. In a WhatsApp message exchange, KONOSHCHENOK is given an order from another individual for “6.5 mm 147 gn – 1000 pcs . . . 6.5 mm 156 gn – 900 pcs . . . 7 mm 190gn – 400 pcs284win – 100 pcs . . . The first three are bullets. The fourth one is casings.”

33. In another message, KONOSHCHENOK sent a WhatsApp message to another individual that his fee is “10%” because he “can't do less. Sanctions . . . Sanction item for 10%,” which I assess to be a reference to KONOSHCHENOK charging a premium fee to ship or transport

goods to sanctioned end-users, for example those on the Entity List or SDN List, because of the risks associated with the potentially unlawful nature of such transport or shipment.

34. To consummate some of their transactions, Livshits advised KONOSHCHENOK to “fabricate” or “draw” the “receipt” and other documents. In one text message, Livshits asked KONOSHCHENOK if he can “send the money to Stonebridge . . . for example for auto parts.” As discussed further below, incident to KONOSHCHENOK’s arrest approximately 375 pounds of ammunition were recovered from a warehouse used by KONOSHCHENOK.

35. Additionally, on or about and between May 2020 and October 2022, Livshits and KONOSHCHENOK had multiple email communications concerning the purchase of electronic items including the following:

a. On May 25, 2020, Livshits wrote to KONOSHCHENOK: “Vadim, You must purchase the following items from the Rivor Store: 92470515 - NextZett Cockpit Premium 500ml - €5.51 - 3 pcs (€16.53)<http://www.rivor.ee/ru/search?page=1&q=9247051592480515> - NextZett Leather Salon Care Product - €9.96 - 1 pc<http://www.rivor.ee/ru/a/nz-produkt-po-uhodu-za-kozhej-250ml> 91110415 - NextZett Klima-Cleaner - €6.50 - 1 pc <http://www.rivor.ee/ru/a/nz-klima-cleaner-klima-ochistitel-100ml> 91391215 - NextZett insect removal - €4.98 - 1 pc <http://www.rivor.ee/ru/a/nz-udalenienasekomyh-i-predvaritel-naja-ochistka-500ml-anti-insekt> 92441015 - NextZett plastic cleaner - €5.27 - 1 pc<http://www.rivor.ee/ru/a/nz-ochistiteldlja-plastika-500ml-plastikreiniger> Total: €43.24 Store contacts: Tel.: +(372) 6 599 620 Väike-Männiku 13, 11216 Tallinn, Eesti AS Rivo.” That same day, KONOSHCHENOK responded: “Good. I’ll buy everything out tomorrow morning.”

b. On July 22, 2020, Livshits wrote to KONOSHCHENOK a list of

“products” and listed a variety of electronic components to be purchased from an Estonian website, <https://www.silver.ee/>.

c. On May 2, 2022, Livshits wrote to KONOSHCHENOK: “Vadim, You must pay the invoice to Foltronics in Holland. Invoice attached. Their bank details and other details are down there. €2,537.00.” Livhsits also included banking information to make the payment.

d. On May 23, 2022, Livshits wrote to KONOSHCHENOK: “Good afternoon, I attach the DHL 4084774886 shipping files to be uploaded to EMTA declaration mail packages (not Impulse). Total of 5 files to upload to EMTA, in the section "Customs Check -> Download Documents": 1.Product photo2. DHL label3. DHL invoice4. Paypal payment receipt5. Product datasheet6. Text file - it must be uploaded to EMTA along with the documents HST/Tariff Code: 8541600000 MRN # check with DHL Tallinn: 680.8525 / tolliosakond@dhl.com Boris.” The next day, Livshits received an import declaration from Timeless Electronics in Israel, listing KONOSHCHENOK’s address in Estonia.

36. Notably, KONOSHCHENOK has also represented that he has a relationship with Russian intelligence. Specifically, in October 2020 WhatsApp messages KONOSHCHENOK identifies himself to an individual as a “Colonel” with the FSB. KONOSHCHENOK’s phone also contained entries reflecting “FSB order[s].” KONOSHCHENOK also enclosed a photograph of himself wearing an FSB uniform in a text message to another person.

V. KONOSHCHENOK’s Use of Physical Premises in Estonia to Further the Conspiracy

37. Evidence gathered pursuant to this investigation revealed that KONOSHCHENOK utilized multiple premises in Estonia as part of the criminal conspiracy, including (1) a location in Narva, Estonia (the “Narva Premises”); (2) a warehouse in Tallinn, Estonia (the “Tallinn Warehouse”) and (3) his personal residence in Tallinn, Estonia (the “Tallinn Residence”).

38. Invoices sent from Livshits to KONOSHCHENOK reflected that 13,262 Euros worth of U.S.-origin sniper ammunition were sent to the Narva Premises. This shipment was mailed from Italy and addressed to “Stonebridge Resources.” One invoice was dated September 29, 2022.

39. According to text messages, Livshits directed KONOSHCHENOK to order an electronic item and have it delivered to the Narva Premises, with the invoice dated September 21, 2022. Additionally, KONOSHCHENOK was in possession of multiple invoices for Stonebridge Resources for export-controlled oscilloscopes, dated between August 2022 and September 2022, all addressed to the Narva Premises. During his border stop on November 24, 2022, the U.S.-origin bullets that were seized were invoiced to Stonebridge Resources and listed the Narva Premises address, dated November 23, 2022. The invoice for the U.S.-origin bullets was in KONOSHCHENOK’s vehicle with him when it was stopped in November 2022.

40. On or about January 7, 2023, after KONOSHCHENOK’s arrest, Estonian authorities stopped a vehicle attempting to travel into Russia, and discovered 7,900 bullets, some of which were manufactured by the same U.S. company whose bullets were shipped to, and found in the possession of, KONOSHCHENOK. According to the driver of the vehicle (“Individual-1”), he was asked to deliver this shipment of bullets by another person (“Individual-2”), who resided at the Narva Premises.

41. Finally, with regard to the Tallinn Residence, shipping records indicate that two export-controlled, U.S.-origin items that were shipped to KONOSHCHENOK’s home address by way of the New Hampshire residence used by Brayman. Additionally, approximately one month before the October 2022 Estonian border stop of KONOSHCHENOK, at least three shipments of ammunition from a German distributor of U.S.-manufactured ammunition were sent to the Tallinn

Residence. This is the same brand of U.S. ammunition that was seized from KONOSHCHENOK's car by Estonian authorities when he was attempting to travel into Russia.

VI. KONOSHCHENOK's Arrest and Seizure of the POST-ARREST DEVICES and PREMISES DEVICES

42. On or about December 6, 2022, KONOSHCHENOK was arrested by Estonian authorities pursuant to a provisional arrest request from the United States.

43. KONOSHCHENOK was found in possession of multiple electronic devices at the time of his arrest, i.e., the POST-ARREST DEVICES. KONOSHCHENOK also provided passwords for the various devices to Estonian authorities.

44. Following his arrest, KONOSHCHENOK made statements to Estonian authorities stating, in sum and substance, that "bullets" were located at a "warehouse in Tallinn" held in the name of KONOSHCHENOK's son.

45. On or about December 6, 2022, after the arrest and with the consent of KONOSHCHENOK's son, Estonian authorities searched the Tallinn Warehouse. The Tallinn Warehouse contained, among other things, six cardboard boxes containing more than 10,000 rounds of ammunition.

46. On or about January 7, 2023, pursuant to an MLAT from the United States, Estonian authorities conducted a search of the Tallinn Residence, as well as a second search of the Tallinn Warehouse.

47. At the Tallinn Warehouse, Estonian authorities observed and/or seized, among other things, a desktop computer; business records including invoices from U.S.-based electronics companies; corporate stamps for Stonebridge Resources; and a copy of the Indictment related to this matter, which was found in a garbage can located near a workstation that was identified as belonging to KONOSHCHENOK.

48. The Tallinn Residence contained, among other things, mail directed to KONOSHCHENOK; multiple Russian passports in KONOSHCHENOK's name, including multiple passports with the passport number and other parts of the passport cut out; a credit or debit card associated with a Russian bank; and multiple sheets of paper containing what appears to be password information. The Tallinn Residence also contained the PREMISES DEVICES.

49. The number of electronic devices found in KONOSCHENOK's possession at the time of his arrest, and at the Tallinn Residence is notable and relevant to probable cause. Based on my training and experience, individuals involved in export control and sanctions evasion schemes will use multiple electronic devices to further the scheme and in an attempt to evade law enforcement detection. This is particularly true where, as is the case here, the individual is involved in a sophisticated scheme that involves complex logistics to move goods across multiple international borders and involves communications with a substantial number of individuals.

50. As discussed above, KONOSHCHENOK used multiple means of electronic communications, including email, WhatsApp and text messaging, to communicate with various members of the conspiracy. Based on my training and experience, I know that individuals who use multiple electronic devices often rely upon cloud computing services and other applications that permit the user to access their information across multiple electronic devices. According to records provided by Apple, KONOSHCHENOK maintained an Apple iCloud account and had iCloud features activated that permitted him to backup data and access that data across multiple devices, including both mobile devices and computers. The WhatsApp messaging service, which KONOSHCHENOK used to send messages to further the scheme, similarly permits users to access their accounts and send messages from multiple mobile devices and computers.

51. On or about December 18, 2023, the SUBJECT DEVICES, along with certain other evidence, were turned over to the FBI by Estonian authorities.

TECHNICAL TERMS

52. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard

drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer

programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, external hard drives, and other magnetic or optical media.

53. Based on my training, experience, and research, I know that the SUBJECT DEVICES have capabilities that variously allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, storage media and/or PDAs. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT DEVICES.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

54. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

55. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

57. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION


58. Based on the forgoing, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Special Agent Nicholas Milan
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable telephonic and electronic means
pursuant to Federal Rule of Criminal Procedure 4.1, this
11th day of January, 2024



THE HONORABLE JOSEPH A. MARUTOLLO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

The property to be searched is:

- (1) One 4 GB Kingston SD Card;
- (2) Six (6) USB flash drives;
- (3) Samsung Galaxy watch with black straps;
- (4) Dell Latitude 5590 laptop, No. 25650703802;
- (5) Seagate external hard drive, P/N IK9AP6-501;
- (6) Samsung model cellphone with IMEI No. 351518945352256/01 and IMEI2 No. 351681915352258/01;
- (7) Apple iPhone with IMEI No. 357631096484234/01 and IMEI2 No. 357632096484232/01;
- (8) Samsung SM-J320FN cellphone with IMEI No. 355099088222438;
- (9) Toshiba Portege R300 Laptop, serial no. 88029479H;
- (10) Cromax X1800 cellphone with IMEI Nos. 911481400403598, 911481400403606, and SIM card Nos. 89701013958022120647 and 897010210953878537;
- (11) Philips Xenium E311 cellphone with IMEI Nos. 866635024442572 and 866635027192570 and Elise SIM card No. EE21220123062206;
- (12) Samsung SM-G920F cellphone with IMEI No. 359937067052258;
- (13) Sony Ericsson LT18i cellphone with IMEI No. 351870057473267;
- (14) Tele2 SIM-card case with IMSI No. 89372038005053487270;
- (15) ZTE-G S202 cellphone with IMEI No. 868663001743653 and ELISA SIM card No. EE21170815376853;
- (16) Silicon Power 4GB SD memory card;
- (17) myPhone 3320 cellphone with IMEI Nos. 354028090104483 and 354028090104491;
- (18) Nokia 8800E-1 cell phone with IMEI No. 358645013721543;
- (19) BQ-3201 cellphone with IMEI Nos. 351614102396465 and 351614102396473, SIM card with IMSI No. 897010210782518668;
- (20) Samsung SM-G925F cell phone with IMEI No. 357460106/573487/8;
- (21) Huawei ATU-L21 cell phone;
- (22) Samsung NP-R509 laptop, serial no. Z9S993FS300637T;
- (23) Acer Aspire 5750 laptop, serial no. LXRL802041 1340187F3400; and

(24) Prestigio MultiPad tablet, serial no. PMP11122405214;

(collectively, the “SUBJECT DEVICES”) that were recovered from the person of VADIM KONOSHCHENOK on or about December 6, 2022, and the residence of VADIM KONOSHCHENOK, located in Tallinn, Estonia, on or about January 7, 2023. The SUBJECT DEVICES are currently in law enforcement possession within the Eastern District of New York.

ATTACHMENT B

Particular Things to be Seized

All information or records on the SUBJECT DEVICES described in Attachment A that relate to violations of the International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1701 et seq.; the Export Control Reform Act (“ECRA”), 50 U.S.C. § 4801 et seq. and related regulations; Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 554 (smuggling goods); Title 18, United States Code, Section 1956 (money laundering); as well as conspiracy to commit such offenses under Title 18, United States Code, Sections 371 and 1349 (collectively, the “Subject Offenses”), committed by or involving VADIM KONOSHCHENOK, since January 1, 2017, including:

- a. Communications or other records between, among, or about KONOSHCHENOK, and other co-conspirators, including individuals whose identities are not yet known, including communications through intermediaries, regarding the Subject Offenses;
- b. Communications or other records between, among, or about academic or scientific researchers, academic or scientific research (including research related to quantum physics, quantum mechanics, and quantum computing), research institutions, funding or payment for research, research being collected or conducted in the United States, or conducting or transferring research or research findings outside of the United States;
- c. Communications or other records between, among, or about officials of universities or research institutions based in Russia, including communications through intermediaries;
- d. Communications or other records between, among, or about individuals or entities or individuals who are employed by or maintain an affiliation with individuals or entities who at any point in time have been placed on the U.S. Department of the Treasury, Office of Foreign Assets Control’s Specially Designated Nationals List;
- e. Communications or other records between, among, or about individuals or entities or individuals who are employed by or maintain an affiliation with individuals or entities who at any point in time have been on the U.S. Department of the Commerce, Bureau of Industry and Security’s Entity List or Military End User List;

- f. Records and other information regarding KONOSHCHENOK and other coconspirators' travel to and from the United States;
- g. Records and other information relating to the physical locations of KONOSHCHENOK and other coconspirators, including Global Positioning System location data, Internet Protocol address information, photographs, videos, audio recordings, and communications;
- h. Copies of documentation or other records from Russian officials or employees or affiliated researchers at academic or research institutions or companies outside of the United States related to the Subject Offenses;
- i. Financial information related to KONOSHCHENOK and other coconspirators' transfer of money, including bank statements, money transfers, tax filings, and communications regarding financial information;
- j. Information relating to knowledge or awareness of law enforcement or government investigations, electronic or physical surveillance by law enforcement, means and methods of evading law enforcement surveillance or of concealing activities from law enforcement or government agencies, and communications discussing whether one or more persons is under surveillance or investigation by law enforcement or government agencies;
- k. Information relating to attempts to alter, destroy, mutilate, or conceal a record, document, or other object, including by destroying physical records, deactivating any Internet account, deleting applications from an electronic device, or concealing an electronic device from law enforcement or other government agencies;
- l. Information relating to any benefit, financial or otherwise, conferred to KONOSHCHENOK, and other co-conspirators for committing the Subject Offenses;
- m. Attribution evidence showing who used or owned the SUBJECT DEVICES at the time the records and information described in this warrant were created, edited, or deleted, including logs, phonebooks, saved usernames and passwords, documents, browsing history, photographs, videos, audio recordings, and messages; and
- n. Evidence indicating the state of mind of KONOSHCHENOK, and other coconspirators, including individuals whose identities are not yet known, as it relates to the crimes under investigation.

As used above, the terms "records" and "information" include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form

(such as printing or typing); and any aural or photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

This warrant authorizes a review of electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, language experts and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.